REMARKS

In the Office Action the Examiner noted that claims 2-4, 7, and 14-21 are pending in the application, and the Examiner rejected all claims. By this Amendment, claims 14-21 have been amended. No new matter has been presented. Thus, claims 2-4, 7, and 14-21 remain pending in the application. The Examiner's rejections are traversed below, and reconsideration of all rejected claims is respectfully requested.

Interview With the Examiner

The Applicants would like to express appreciation to the Examiner for the interview granted by the Examiner on December 28, 2006, and the several conversations since that date. During these discussions, the Applicants presented features of the claimed invention which the Applicants feel are not disclosed or suggested by the cited references. At least portions of those arguments, which were also submitted in the Response filed on May 30, 2006, are included in the following remarks.

Claim Rejections Under 35 USC §103

In item 1 on pages 2-5 of the Office Action the Examiner rejected claims 2-4, 7, and 14-21 under 35 U.S.C. §102(a) as being unpatentable over U.S. Patent No. 5,903,652, issued to Mital (hereinafter referred to as "Mital") in view of U.S. Patent No. 5,890,136, issued to Kipp (hereinafter referred to as "Kipp"). The Applicants respectfully traverse the Examiner's rejections of these claims.

Mital discloses a method in which providers of publicly accessible networks are given the capability of monitoring the transmittal of secure documents to ensure proper routing, proper billing, and the proper retrieval of secure documents from backup facilities (Column 3, Lines 10-15). This is done by allowing the system, as essentially a "middle man", to decrypt audit information, which is used as identification information, to allow the system to identify, store, and retrieve the secure document without being aware of the contents of the secure document (Column 5, Lines 26-33). As far as the users of the system of Mital, each of two users generates a pair of a public key and a private key, and transmits one's public key to the other user. The first user may then encrypt a document using the public key of the second user, and send the encrypted document to the second user. The second user may then decrypt the received encrypted document using the second user's private key. A digital signature of the first user may

also be incorporated into the encrypted document, which would be checked by the second user according to a relationship between the encrypted digital signature and the first user's public key (Column 1, Line 61 through Column 2, Line 62).

The Examiner has apparently equated the public and private keys generated and used by the two users as anticipating at least some of the features of the present claimed invention. However, since each of the two users in Mital generates his or her own keys, there are two entities from which the keys originate. This is in direct contrast to the claimed invention, in which there are at least two users in addition to an authentication system. Further, there is only one entity, the authentication system, from which the matching keys of the claimed invention originates, because the matching keys are issued from the authentication system to the two users. In at least this manner, the configuration of Mital is altogether different from the configuration of the claimed invention. This, as well as other aspects in which the claimed invention patentably distinguishes over the cited references, will be further explained below in reference to the claimed features of the present application.

Claim 14 of the present application recites "checking, at an authentication system in response to accesses to the authentication system from terminal devices of the users, whether each of the users satisfies conditions for conducting a prospective transaction." In other words, the authentication system checks whether or not each of the users has the ability to enter into the transaction. As an example of one embodiment only, it may be determined whether or not a buyer is authorized to purchase merchandise, and whether a seller is authorized to sell the merchandise (disclosed in at least Lines 1-18 on page 6 of the present application).

The Examiner stated that this feature is disclosed by the auditing functions of Mital (Abstract; Column 3, Lines 40-53; Column 4, Lines 27-60; and Column 5, Lines 14-25). However, the use of the audit information of Mital simply allows the network service provider to decrypt identification information which allows the electronic commerce service to provide backup copies in the event of a system crash or power outage (Column 5, Lines 14-25). Information regarding the order itself, and payment information, remains encrypted and not read by the electronic commerce service. "Advantageously, the decrypted audit information allows the electronic commerce service to route the encrypted transaction packet while maintaining confidentiality about the specific items and payment instructions" (Column 5, Lines 29-32).

Therefore, Mital does not disclose or suggest checking whether of the users satisfies conditions for conducting a prospective transaction, as is recited in claim 14 of the present application. Mital merely discloses storing identification information to be used in case of a

transaction message not reaching its intended target. Further, Mital is incapable of checking whether both users would be able to enter the transaction, because the transaction information itself is encrypted and not able to be read by the electronic commerce service.

Claim 14 of the present application, as amended, also recites "selecting identical transaction keys on screens of the terminal devices; generating different matching keys based on the identical transaction keys; [and] transmitting the respective different matching keys from the authentication system to the terminal devices." In other words, each of the users are provided with separate respective matching keys from the authentication system, with which a matching function may be performed (disclosed in at least Lines 2-16 on page 8 of the present application).

The Examiner stated that this feature of claim 14 is disclosed by the email module functions of Mital (Column 2, Line 40 to Column 3, Line 20; Column 4, Lines 56-61; and Column 12, Line 50 to Column 13, Line 8). The Examiner is apparently merely citing the act of encrypting an order and sending the encrypted order to a merchant as anticipating this feature of claim 14. However, in the encryption method disclosed in Mital, each of the users creates his or her own public and private key pairs, the key pairs are not generated and transmitted from an authentication system (Column 2, Lines 40-54), which is in direct contrast to claim 14 of the present application. Further, the public and private key pairs of Mital are created at the request of a user with no bearing on whether another user is involved (Column 2, Lines 3-16), much less according to whether or not each of the users satisfies conditions for conducting a prospective transaction, as is recited in claim 14. Mital does not even contemplate the selection of identical transaction keys on the screens of the terminal devices. Further still, therefore, the public and private keys of Mital are not at all related to being generated based on identical transaction keys selected by each of the users.

Claim 14 of the present application also recites "inputting, into a given one of the terminal devices, one of the matching keys that has been transmitted to and received by another one of the terminal devices." As Mital does not disclose or suggest the matching keys being generated and issued from an authentication system, Mital cannot disclose or suggest inputting one of the matching keys, which has been received by a second terminal, into a first terminal. The Examiner is apparently equating this feature of claim 14 with the action in Mital when a first user generates a public and private key, and then transmits the public key to a second user so that the second user can use the public key to send secure documents to the first user. However, as explained in Mital (Column 1, Line 51, through Column 2, Line 62), the public and private key of

the first user is generated locally by the first user. Thus, there are no different matching keys which have been generated and transmitted to both users from an authentication system, and therefore no matching key sent to a first terminal to be input into a second terminal.

Claim 14 of the present application also recites "transmitting said one of the matching keys from said given one of the terminal devices to the authentication system." Again, the Examiner has apparently equated the encryption system of Mital with this feature of claim 14. However, as disclosed by Mital, the decryption of the documents by the user is done locally at the user's computer, and therefore there would be no reason to transmit a matching key from the user's computer to an authentication system. Further, the electronic commerce system of Mital is not able to decrypt the contents of the secure document, so nothing could be accomplished by sending any sort of matching key to the system. The Applicants respectfully submit that this makes any comparison of the present invention to the encryption/decryption system of Mital invalid.

Claim 14 of the present application also recites "checking, at the authentication system, whether said one of the matching keys matches one of the transmitted matching keys." As previously discussed in this Response, the electronic commerce system of Mital is not able to decrypt the content of the secured documents transmitted (the system can only decrypt the identification information termed the "audit information"). Therefore, Mital performs no checking of matching keys at an authentication system. The Examiner has again equated the encryption system of Mital with this feature of claim 14. However, it is apparent that the comparison of the digitally signed portion of the encrypted document is done locally at "Doug's" computer (Column 2, Lines 23-38), and is not done at an authentication system. During the Examiner interview conducted on May 18, 2006, the Examiner compared the issuing of the public and private keys by an encryption service to the authentication system of the present claimed invention. However, the Applicants respectfully submit that the Examiner has already identified the electronic commerce system of Mital as the authentication system, and not an encryption service. And, as explained previously in this Response, the electronic commerce system is not able to decrypt the content of the order information, and therefore is not involved with any sort of matching keys. This also precludes Mital from disclosing the feature of "notifying said one of the terminal devices a result of the checking of the matching keys," also recited in claim 14 of the present application.

Thus, according to at least the reasons presented above, the Applicants respectfully submit that Mital does not disclose any of the features of claim 14 of the present application, and that claim 14 patentably distinguishes over Mital.

The Examiner acknowledged that "Mital does not explicitly disclose if identical transaction keys are selected on screens of the terminal devices and if each of the users satisfies the conditions, said different matching keys being generated based on the identical transaction keys." But the Examiner went on to state that Kipp discloses this feature in the description of automatically verifying the customer identification to release goods for a proper customer (Figure 2; Figure 3 #108; Figure 4 #112, 114, 116, and 118; and Column 6, Line 39 through Column 7, Line 64). This portion of the specification of Kipp, however, only discloses a customer authentication in which a customer is authenticated in the same manner as in a typical purchase using a credit card. That is, a customer is authenticated based on his or her credit card, and merchandise is handed to the customer upon successful authentication. Thus, Kipp only discloses a relationship between the customer identification station and a single customer, and does not teach or suggest the relationship between an authentication system (customer identification system) and two users, as recited in claim 14. In other words, Kipp neither discloses nor suggests selecting identical transaction keys on the different terminals of the two users. Further, in the specification of Kipp, there is no mention of issuing matching keys to the two customers, so there could be no different matching keys generated based on the identical transaction keys, as recited in claim 14.

Therefore, Kipp does not cure the deficiency of Mital regarding the feature discussed by the Examiner. Further, the Applicants respectfully submit that Mital does not disclose any of the features of claim 14 of the present application. To form a proper §103 rejection, the cited references must combine to disclose or suggest all of the features of the rejected claim. As shown in this Response, the cited references apparently neither disclose nor suggest any of the recited features of claim 14. Therefore, the Applicants respectfully submit that claim 14 of the present application patentably distinguishes over the cited references.

The Applicants further respectfully submit that there is no motivation to combine Mital and Kipp. Mital is directed to solving the problem of an electronic commerce system not being able to identify secured documents which are lost during routing of online orders, and includes provisions for sending encrypted payment information to the proper "acquirer", or credit company associated with a credit account (Column 8, Lines 43-56 of Mital). Thus, there would be no motivation for one skilled in the art to incorporate the disclosure of Kipp into the method of Mital.

The Applicants respectfully submit that, as there is no motivation for the combination of Mital and Kipp, any §103 rejection based on the combination of the references is improper.

As shown above, claim 14 patentably distinguishes over the cited references. Further, claims 2-4 depend from claim 14 and include all of the features of that claim plus additional features which are not disclosed or suggested by the cited references. Therefore, it is respectfully submitted that claims 2-4 also patentably distinguish over the cited references.

Claims 7 and 15-21 also recited similar features to those discussed in regard to claim 14, and which are not disclosed or suggested by the cited references. Therefore, it is respectfully submitted that claims 7 and 15-21 also patentably distinguish over the cited references.

Summary

In accordance with the foregoing, claims 14-21 have been amended. No new matter has been presented. Thus, claims 2-4, 7, and 14-21 remain pending in the application.

There being no further outstanding objections or rejections, it is respectfully submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

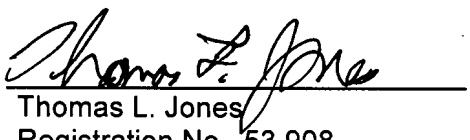
Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: April 5, 2007

By: 

Thomas L. Jones
Registration No. 53,908

1201 New York Avenue, NW, 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501